Naciones Unidas A/66/152

Asamblea General

Distr. general
15 de julio de 2011
Español
Original: inglés/ruso

Sexagésimo sexto período de sesiones
Tema 93 del programa provisional*
Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

Informe del Secretario General

Índice

* A/66/150.

11-41694 (S) 010811 030811

I. Introducción

1. En el párrafo 3 de su resolución 65/41, la Asamblea General invitó a todos los Estados Miembros a que, teniendo en cuenta las evaluaciones y recomendaciones que figuran en el informe del Grupo de Expertos Gubernamentales sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la Internacional seguridad[1], siguieran comunicando al Secretario General sus opiniones y observaciones sobre las cuestiones siguientes:

a) La evaluación general de los problemas de la seguridad de la información;

b) Las medidas que se adoptan a nivel nacional para fortalecer la seguridad de la información y contribuir a la colaboración internacional en ese ámbito;

c) El contenido de los conceptos mencionados en el párrafo 2 de la resolución;

d) Las medidas que la comunidad internacional podría adoptar para fortalecer la seguridad de la información a escala mundial.

2. Atendiendo a esa petición, el 16 de marzo de 2011 se envió una nota verbal a los Estados Miembros para invitarles a proporcionar información sobre el tema. Las respuestas recibidas se recogen en la sección II. Las respuestas que se reciban posteriormente se publicarán como adiciones al presente informe.

II. Respuestas recibidas de los gobiernos

Alemania

[Original: inglés]
[6 de junio de 2011]

La situación de la seguridad en el ciberespacio ha cambiado radicalmente en los últimos años. Por un lado, se puede apreciar cómo funciona un proceso impulsado por la tecnología de la innovación, pues cada vez más los procesos comerciales se gestionan electrónicamente y se conectan entre sí, a veces, directa o indirectamente por conducto de Internet. Los sistemas de la tecnología de la información se vuelven constantemente más complejos. Los ciclos de innovación son cada vez más cortos. Por otro lado, se asiste a ataques de redes y bases de datos informáticas y sitios web por parte de la delincuencia organizada y otros agentes no estatales. En algunos casos, aún no se han evaluado de forma realista los efectos de esos ataques.

Por esta razón, en febrero de 2011 el Gobierno Federal adoptó una nueva estrategia de seguridad cibernética. El núcleo de esta estrategia es la protección de la infraestructura crítica. Todas las autoridades gubernamentales que se ocupan de cuestiones de seguridad cibernética colaboran estrecha y directamente entre sí y con el sector privado en el marco de un nuevo Centro de respuesta cibernético, para detectar y analizar rápidamente los principales incidentes en el ámbito de la tecnología de la información, y recomendar medidas de protección. En materia de política, el nuevo Consejo de seguridad cibernética, que tiene nivel de secretaría de

[1] A/65/201.

Estado, aborda los principales problemas de seguridad cibernética y la posición de Alemania al respecto.

Ello incluye la coordinación de la política exterior en materia cibernética, incluidos aspectos como política exterior, defensa, economía y seguridad. Las interconexiones internacionales en el ciberespacio imponen como factor esencial una acción coordinada a nivel internacional. Por lo tanto, dentro de la Unión Europea y en los organismos internacionales, Alemania ha de promover fervorosamente una mayor seguridad cibernética.

En su estrategia de seguridad cibernética, dado el carácter de interconexión mundial de la tecnología de la información, Alemania aboga por que se elaboren normas de conducta del Estado en el ciberespacio, que sean amplias, no contenciosas y políticamente vinculantes. Deben ser aceptables para una gran parte de la comunidad internacional e incluir medidas para fomentar la confianza y aumentar la seguridad.

Medidas de fomento de la confianza y la seguridad en el ciberespacio

El ciberespacio es un bien público y un espacio público. Como tal, la seguridad del ciberespacio se debe considerar en términos de resistencia de la infraestructura, así como protección de la integridad y seguridad de los sistemas y datos contra fallos. Al ser un espacio público, los Estados tienen que promover la seguridad en el ciberespacio, en particular en lo que respecta a la protección contra la ciberdelincuencia y las actividades malintencionadas, amparando a los que optan por utilizar medios de confirmación de autenticidad contra la suplantación de identidad, y asegurando la integridad y la confidencialidad de los datos y las redes.

El ciberespacio es de índole global. La garantía de la seguridad cibernética, la aplicación efectiva de los derechos y la protección de infraestructuras críticas de la información requieren un gran esfuerzo del Estado, a nivel nacional y en cooperación con socios internacionales.

En este contexto, Alemania está dispuesta a elaborar un conjunto de normas de conducta que aborden el comportamiento de un Estado hacia otro Estado en el ciberespacio, que incluyan en particular medidas de fomento de la confianza, la transparencia y la seguridad, y velar por que sean suscritas por el mayor número posible de países.

Recientemente, en la conferencia de la Organización para la Seguridad y la Cooperación en Europa sobre seguridad cibernética, celebrada los días 9 y 10 de mayo de 2011, Alemania señaló algunos posibles elementos de las normas internacionales de un código de conducta sobre seguridad del espacio cibernético, como los siguientes:

a) Confirmación de los principios generales de disponibilidad, confidencialidad, competitividad, integridad y autenticidad de los datos y las redes, y privacidad y protección de los derechos de propiedad intelectual;

b) Respeto de la obligación de proteger las infraestructuras críticas;

c) Mejoramiento de la cooperación, con miras a fomentar la confianza, adoptar medidas de reducción del riesgo y promover la transparencia y la estabilidad, mediante:

- El intercambio de estrategias nacionales, mejores prácticas y percepciones nacionales referentes a la reglamentación internacional del ciberespacio,
- El intercambio de puntos de vista nacionales acerca de las normas jurídicas internacionales relativas al uso del ciberespacio,
- La configuración y notificación de puntos de contacto,
- El establecimiento de mecanismos de alerta temprana y el fortalecimiento de la cooperación, entre otras cosas, entre los equipos de respuesta ante emergencias informáticas,
- La actualización de los enlaces de comunicación en situaciones de crisis, para abarcar los incidentes cibernéticos, y el apoyo a la elaboración de recomendaciones técnicas que promuevan infraestructuras cibernéticas mundiales robustas y seguras,
- La responsabilidad de luchar contra el terrorismo, que incluye el intercambio de prácticas y una mayor cooperación para hacer frente a los actores no estatales,
- La asistencia para la creación de capacidad en materia de seguridad cibernética en los países en desarrollo, y el establecimiento de medidas voluntarias en apoyo de la seguridad cibernética para acontecimientos de gran escala, por ejemplo, los Juegos Olímpicos.

Por otra parte, percibimos la necesidad de iniciar un debate sobre una cooperación internacional en el marco de la atribución de los ataques cibernéticos, que suelen ser muy difíciles de rastrear, la responsabilidad del Estado por los ataques cibernéticos lanzados desde su territorio, cuando los Estados no hacen nada para poner fin a estos ataques a pesar de estar informados acerca de ellos, y la responsabilidad de los Estados de no facilitar zonas de ilegalidad en el ciberespacio, por ejemplo, tolerar a sabiendas el almacenamiento de datos personales recogidos ilegalmente en su territorio.

Aspectos militares de la seguridad cibernética

A medida de que las fuerzas militares dependen cada vez más de la tecnología de la información para llegar a dominar hipótesis cada vez más complejas en todos los niveles de mando, la protección de la información y los medios para procesarla se han convertido en una tarea de primer orden.

Sin embargo, en el pensamiento militar, las amenazas a la seguridad de información proceden no sólo por un adversario potencial, en el sentido operacional, con utilización de armas para la destrucción física de la infraestructura de información, sino también de los usuarios irresponsables, el mal funcionamiento de la tecnología, los delincuentes o simplemente los accidentes.

Por lo tanto, los esfuerzos que deben emprenderse varían desde sensibilizar a cada usuario y asegurar la fiabilidad de la cadena de oferta de tecnología de la información, hasta poner en práctica formas de respuesta para defenderse de los ataques cibernéticos y establecer una arquitectura general de la tecnología de la información que sea resistente.

En esencia, es necesaria una gestión integral del riesgo, con medidas para reforzar la seguridad de la información a escala nacional y global.

Las fuerzas armadas alemanas (Bundeswehr) han establecido arquitecturas de mando y de control resistentes, técnicas y procedimientos de seguridad, así como una organización de seguridad de la tecnología de la información que incorpora a todas las secciones de las fuerzas armadas, incluido un equipo de respuesta ante emergencias informáticas independiente, con capacidad para intervenir en caso de perturbaciones críticas del funcionamiento de la tecnología de la información. Adaptar las aptitudes personales y técnicas al constante aumento del nivel de la amenaza es una tarea permanente.

Las fuerzas armadas alemanas colaboran estrechamente con el Ministerio del Interior Federal de Alemania en sus esfuerzos, y apoyan firmemente el fortalecimiento de la seguridad de la información en la Organización del Tratado del Atlántico Norte (OTAN) y la UE y la formación de políticas y capacidades a ese efecto. Además, las fuerzas armadas mantienen intercambios regulares con un número de países en el contexto de seguridad de la información a nivel normativo y operacional.

Las fuerzas armadas alemanas acogen con satisfacción las iniciativas y trabajan en conjunto con otros departamentos del Gobierno Federal de Alemania sobre propuestas internacionales para proteger aún más la utilidad de las redes de información en el plano mundial, por ejemplo, la elaboración de un código internacional de conducta en el ciberespacio, de carácter voluntario.

Defensa del espacio cibernético en la OTAN

La OTAN ha determinado que la seguridad del espacio cibernético es uno de los nuevos ámbitos que surgen en materia de amenazas a la seguridad. El concepto estratégico adoptado por los Jefes de Estado y de Gobierno en la Cumbre de la OTAN celebrada el 20 de noviembre de 2010 en Lisboa indica que “los ciberataques pueden llegar a un umbral que amenace la prosperidad, la seguridad y la estabilidad nacional y euroatlántica”.

En la Declaración de la Cumbre, los Jefes de Estado y de Gobierno encomendaron al Consejo del Atlántico Norte que “elabore, basándose sobre todo en las estructuras internacionales existentes y sobre la base de una revisión de nuestra política actual, una política de ciberdefensa en profundidad de la OTAN, antes de junio de 2011 y prepare un plan de acción para su aplicación”.

Como primer paso hacia la nueva política, en marzo de 2011 los Ministros de Defensa de la OTAN adoptaron un concepto de defensa del espacio cibernético.

El concepto se centra en la protección de las redes de la OTAN y las redes nacionales de los Estados miembros que están conectadas a las redes de la OTAN o procesan información de la Alianza (lo que incluye la elaboración de principios y criterios comunes para garantizar un nivel mínimo de defensa del ciberespacio en todos los Estados miembros). Para reducir los riesgos globales que emanan del espacio cibernético, la OTAN tiene la intención de cooperar con los países socios, los órganos internacionales pertinentes, como las Naciones Unidas y la Unión Europea, el sector privado y los círculos académicos.

Alemania celebra el compromiso de la OTAN en materia de seguridad cibernética y apoya activamente las deliberaciones al respecto.

Seguridad cibernética en la Organización de la Seguridad y la Cooperación en Europa

La Organización de la Seguridad y la Cooperación en Europa examina los problemas de la "seguridad cibernética" desde hace varios años. En la Cumbre de la OSCE celebrada en 2010 en Astana, los Jefes de Estado y de Gobierno de los 56 Estados participantes en la OSCE subrayaron que se debía lograr una mayor unidad de propósito y de actuación para hacer frente a las nuevas amenazas transnacionales. La Declaración conmemorativa de Astana mencionó las "ciberamenazas" como una de estas nuevas amenazas transnacionales.

Alemania participó activamente en la Conferencia de la OSCE sobre un enfoque integral de la seguridad cibernética: "Análisis del papel de la OSCE en el futuro", celebrada los días 9 y 10 de mayo de 2011 en Viena. En el transcurso de la conferencia, se examinaron recomendaciones concretas para el seguimiento de las actividades de la OSCE.

Alemania seguirá apoyando activamente los debates de la OSCE sobre un análisis del papel de la OSCE en el ámbito de la seguridad cibernética en el futuro.

Australia

[Original: inglés]
[31 de mayo de 2011]

Australia agradece la oportunidad de presentar esta respuesta, que contiene nuestros puntos de vista en cumplimiento de la resolución 65/41 de la Asamblea General, sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional.

Australia aspira a ser un líder mundial en seguridad cibernética. Reconocemos la importancia y los beneficios de los avances en la tecnología para la economía digital global y la seguridad de todas las naciones. Australia tiene como objetivo aumentar al máximo el beneficio económico y en términos de seguridad que resulte de nuestra experiencia, para todas las naciones.

A medida que las tecnologías han penetrado gradualmente en nuestra vida, el gobierno, las empresas y los particulares dependen cada vez más de ellas para una variedad de propósitos y funciones, que varían entre comprar en línea bienes y servicios, comunicarse con los demás, buscar información y administrar las finanzas y controlar equipos en las industrias de extracción y manufacturera. Para sacar el máximo provecho de Internet y de la economía digital, y mejorar la seguridad cibernética en todo el mundo, es imperativo que las naciones trabajen juntas para lograr un ciberespacio fiable, seguro y resistente. Australia se esfuerza por trabajar de forma activa y comprometida en el mejoramiento del espacio cibernético para todos los usuarios, ya sean Estados, empresas o particulares.

Evaluación general de los problemas de la seguridad de la información

Australia reconoce que la seguridad del ciberespacio es una prioridad a nivel de la seguridad nacional. La comunidad internacional continúa experimentando un aumento en la escala, sofisticación y éxito de la ciberdelincuencia. A medida que ha

aumentado la cantidad y el valor de la información electrónica, también se han intensificado los esfuerzos de los delincuentes y otros agentes malintencionados que han adoptado Internet como una forma más anónima, conveniente y rentable de llevar a cabo sus actividades.

El tratamiento y la gestión de estos riesgos se deben sopesar en relación con las libertades civiles individuales, incluido el derecho a la privacidad, y la necesidad de promover la eficiencia y la innovación para asegurar que Australia aproveche plenamente el potencial de la economía digital.

La seguridad nacional, la prosperidad económica y el bienestar social de Australia, y de toda nación, dependen fundamentalmente de la disponibilidad, integridad y confidencialidad de una amplia gama de tecnologías de la información y las comunicaciones. Atendiendo a esta circunstancia, el Gobierno australiano ha dedicado importantes recursos a promover activamente el mantenimiento de un entorno electrónico operacional fiable, seguro y resistente para el beneficio de todos los usuarios.

La política de seguridad cibernética del Gobierno de Australia, si bien se refiere principalmente a la disponibilidad, integridad y confidencialidad de las tecnologías de la información y las comunicaciones del país, está coordinada con otras políticas y programas relacionados, tales como la protección cibernética, que se centra en amparar a las personas, especialmente los niños, de los contenidos ofensivos, la intimidación, el acoso o la manipulación en línea para fines de explotación sexual.

Medidas que se adoptan a nivel nacional para fortalecer la seguridad de la información y contribuir a la colaboración internacional en ese ámbito

Medidas que se adoptan a nivel nacional para fortalecer la seguridad de la información

Australia reconoce que debe configurar mejores prácticas a nivel nacional para poder promover la cooperación internacional en el ciberespacio. El país ha adoptado un enfoque integrado y dirigido por el gobierno para proteger y fortalecer la seguridad cibernética. En 2009, el Gobierno dio a conocer su primera estrategia de seguridad cibernética, que articula la finalidad y los objetivos generales de la política de la seguridad cibernética de las autoridades y establece las prioridades estratégicas que aplicará para lograr estos objetivos. La estrategia también describe las acciones y medidas clave que se ejecutarán como parte de las tareas exhaustivas en todos los sectores de la administración de Australia para la consecución de esas prioridades estratégicas.

El objetivo de la política de seguridad cibernética de Australia es mantener un entorno electrónico operacional fiable, seguro y resistente que apoye la seguridad nacional del país y eleve al máximo los beneficios de la economía digital. Entre las iniciativas clave de la estrategia se pueden mencionar la creación de dos organizaciones que se apoyan mutuamente, a saber, un nuevo equipo nacional de respuesta ante emergencias informáticas y el Centro de operaciones de seguridad cibernética. Fundado en 2010, el equipo nacional de Australia ofrece un punto de contacto único para obtener información de seguridad cibernética para todos los habitantes y empresas australianas, y garantiza que los usuarios de Internet en el país

tengan acceso a la información sobre amenazas cibernéticas, la vulnerabilidad de sus sistemas e información sobre cómo proteger mejor sus tecnologías de la información y las comunicaciones. El equipo mantiene estrechas relaciones de trabajo con los propietarios y operadores de infraestructuras y las empresas que explotan sistemas importantes para el interés nacional de Australia. Proporciona a estas empresas información seleccionada sobre las amenazas a la seguridad cibernética y la vulnerabilidad, para ayudarlas a proteger mejor su infraestructura tecnológica. El Centro de operaciones de seguridad cibernética, también establecido en 2010, ofrece al Gobierno de Australia conocimientos de la situación procedentes de todas las fuentes, y una mayor capacidad para facilitar respuestas operacionales a los incidentes de seguridad cibernética de importancia nacional. El Centro identifica y analiza los ataques cibernéticos complejos, y ayuda a responder a los incidentes cibernéticos en los sistemas e infraestructuras esenciales del Gobierno y del sector privado por igual.

Una de las prioridades clave de la estrategia consiste en educar y capacitar a todos los australianos, proporcionándoles información, fomentando la confianza y dotándolos de herramientas prácticas para protegerse en línea. La estrategia se orienta por el principio de responsabilidad compartida, en virtud del cual todos los usuarios, al aprovechar los beneficios de las tecnologías de la información y las comunicaciones, deben tomar medidas razonables para proteger sus propios sistemas, obrar con prudencia en sus actividades de comunicación y almacenamiento de información delicada y respetar la información y los sistemas de otros usuarios. Para que las personas puedan desempeñar un papel activo en la seguridad de la información, es esencial que conozcan y comprendan en todo momento el entorno cibernético y sus riesgos. Para lograrlo, Australia aplica un programa continuo de sensibilización, que incluye un sitio web con información sobre seguridad cibernética para los usuarios domésticos y pequeñas empresas del país, incluidos los que tienen escasos conocimientos y aptitudes informáticos (véase www.staysmartonline.gov.au) y ha instituido una Semana nacional de sensibilización sobre seguridad cibernética, en colaboración con empresas, grupos de consumidores, y organizaciones comunitarias. La Semana nacional de sensibilización ayuda a la población a entender los riesgos de la seguridad cibernética y enseña a los usuarios domésticos y las pequeñas empresas medidas sencillas que pueden adoptar para proteger su información personal y financiera en línea. Durante la edición de 2010 de la Semana nacional de sensibilización sobre seguridad cibernética, alrededor de 150 agencias gubernamentales, la industria y organizaciones de la comunidad y de consumidores se asociaron para ofrecer eventos y actividades en las zonas metropolitana, regional y rural de Australia. En 2011, la Semana nacional de sensibilización se celebrará del 30 de mayo al 4 de junio.

Reconociendo que la seguridad del espacio cibernético es una responsabilidad compartida, el Gobierno de Australia ha trabajado activamente con la Asociación de la industria de Internet para elaborar un innovador código de práctica de seguridad cibernética para proveedores de servicios Internet (el “iCode”), de carácter voluntario, que comenzó su vigencia en diciembre de 2010. El iCode ofrece a los proveedores de servicios Internet de Australia un enfoque coherente para que puedan informar, educar y proteger a sus clientes en relación con las cuestiones de seguridad cibernética. Australia ha hecho una presentación sobre los buenos resultados obtenidos con el iCode y ha compartido las lecciones aprendidas en la elaboración de este instrumento en foros multilaterales. Se han presentado ponencias en el Grupo de Trabajo sobre seguridad de la información y privacidad,

de la Organización de Cooperación y Desarrollo Económicos, en diciembre de 2010, el Grupo de Trabajo sobre información y telecomunicaciones, del Foro de Cooperación Económica de Asia-Pacífico (APEC) y la Telecomunidad de Asia-Pacífico (APT). Australia está dispuesta a compartir este código con otros Estados, a través de actividades de fomento de la capacidad bilaterales y foros multilaterales, para ayudarles a colaborar mejor con los proveedores de Internet e inculcarles en mayor grado su responsabilidad de educar y proteger a los usuarios finales.

Promoción de la cooperación internacional

Australia otorga una alta prioridad a la cooperación internacional en materia de seguridad cibernética. Dado el carácter transnacional de Internet, una seguridad cibernética efectiva requiere una acción coordinada a nivel mundial, y Australia ha asumido su compromiso internacional a través de un enfoque activo y distribuido en múltiples estratos. Éste incluye, entre otras cosas, dialogar con gobiernos extranjeros y organizaciones a nivel bilateral y a través de foros multilaterales, para ayudar a promover las mejores prácticas internacionales, compartir las enseñanzas aprendidas, crear capacidad y fomentar un enfoque global coordinado para combatir las amenazas a la seguridad cibernética.

La participación de Australia en las Naciones Unidas incluye su copatrocinio de resoluciones sobre la creación de una cultura mundial de la seguridad cibernética y el inventario de los esfuerzos nacionales para proteger las infraestructuras críticas de la información, y sobre los avances en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional. Australia también ha respondido a la resolución 64/211 de la Asamblea General ofreciendo su contribución acerca de las mejores prácticas para la protección de las infraestructuras críticas de información, incluidas las tecnologías de la información y las comunicaciones, con miras a fomentar un mejoramiento global de la seguridad cibernética. Australia es miembro de la Unión Internacional de Telecomunicaciones (UIT), y contribuye a las Comisiones de Estudio de los Sectores de Normalización y de Desarrollo. El país aporta financiación al Sector de Desarrollo para la labor de fomento de capacidad en la región de Asia y el Pacífico, lo que incluye iniciativas de seguridad cibernética. Australia es un activo colaborador y anterior titular de la Presidencia del Grupo de Trabajo de la OCDE sobre la seguridad de la información y la privacidad, y es actualmente uno de los países que se han ofrecido como voluntarios para el análisis comparativo de las estrategias de seguridad cibernética por parte del Grupo de Trabajo. Australia ofreció una aportación fundamental en la elaboración y aplicación del Acuerdo de Seúl-Melbourne contra el envío masivo de mensajes no solicitados, relativo a la cooperación entre las naciones de Asia y el Pacífico en la lucha contra tales envíos masivos y el Plan de Acción de Londres, que es la principal red internacional de cooperación para la lucha efectiva contra este fenómeno.

Australia mantiene una relación de colaboración con sus socios regionales y está resuelta a trabajar con ellos. Mantenemos un diálogo muy estrecho con los demás países de nuestra región para el fomento de capacidades necesarias con miras a lograr un ciberespacio fiable, resistente y seguro. Australia participa en las actividades del Grupo de Trabajo sobre información y telecomunicaciones del Foro de Cooperación Económica de Asia-Pacífico (APEC TEL) y los trabajos del Foro Regional de la Asociación de Naciones del Asia Sudoriental (ASEAN) sobre seguridad cibernética. Es también coordinador adjunto del Grupo Directivo de seguridad y prosperidad de APEC TEL. El país actualmente pretende asumir la

dirección conjunta del ámbito central del terrorismo cibernético y la delincuencia transnacional en el marco del Plan de Trabajo del Foro Regional de la ASEAN.

A nivel operativo, el equipo nacional de respuesta ante emergencias de Australia mantiene relaciones de trabajo estrechas con las organizaciones que nuclean a otros equipos similares en todo el mundo. En Australia, el equipo participa activamente y facilita un intercambio fiable y oportuno de información a nivel mundial, lo que incluye información sobre amenazas y vulnerabilidad, para garantizar un conocimiento de la situación y una respuesta mundial coherente y coordinada a las amenazas en línea. El equipo contribuye activamente a las iniciativas de fomento de la capacidad, particularmente en la región de Asia y el Pacífico, incluso mediante su participación en el equipo respuesta de emergencias informáticas de esa región. Reconociendo que la seguridad de la información no está limitada geográficamente, el equipo también trabaja en estrecha colaboración con otros socios, en su calidad de miembro del Foro de equipos de seguridad y de respuesta a incidentes y la Red de alerta y vigilancia internacional.

Posibles medidas que podría adoptar la comunidad internacional para fortalecer la seguridad de la información a nivel mundial

Todos los Estados, entre ellos Australia, deben seguir buscando medidas tradicionales e innovadoras para fortalecer la seguridad de la información. El desafío mundial de la seguridad cibernética requiere un mayor esfuerzo en los foros multilaterales para mejorar la seguridad de las redes interconectadas. Con ello se alude a los esfuerzos de las Naciones Unidas y la UIT, y los foros regionales como APEC y grupos internacionales temáticos más específicos, como el Foro de equipos de seguridad y de respuesta a incidentes y la Red de alerta y vigilancia internacional.

Australia apoya la elaboración de principios internacionales para una conducta responsable en el ciberespacio, en particular, un acuerdo sobre un amplio conjunto de principios para una conducta reglamentada en ese ámbito, que facilite una mejor cooperación internacional y promueva la confianza en el espacio cibernético, y permita la elaboración de normas internacionales acordadas sobre las actividades en esa esfera. Australia, como miembro de la comunidad internacional, seguirá apoyando los avances que se hagan en la cuestión a través de los foros bilaterales y multilaterales, como contribución al logro de un entorno cibernético más seguro, resistente y fiable.

Las medidas específicas que podrían adoptar la comunidad internacional para fortalecer la seguridad de la información a nivel mundial son:

a) La elaboración de normas globales, incluido un acuerdo sobre un amplio conjunto de principios internacionales para la conducta normativa en el ciberespacio, a fin de facilitar la cooperación internacional y promover la confianza;

b) La expansión del alcance del sistema jurídico internacional para combatir la ciberdelincuencia, incluida la coherencia de los marcos jurídicos (por ejemplo, una mayor adhesión al Convenio sobre la Ciberdelincuencia, del Consejo de Europa, cuyos requisitos Australia prevé que podrá cumplir a finales de 2011), y una mejor cooperación en materia de observancia de la ley, para que los países puedan establecer efectivamente una legislación nacional;

c) El desarrollo y la promoción de mejores prácticas, un conocimiento de la situación y una respuesta estratégica a las alertas e incidentes, en particular el establecimiento de equipos nacionales de respuesta ante las emergencias informáticas, para ejecutar y coordinar las actividades entre todas las naciones;

d) Iniciativas de sensibilización y ejercicios de fomento de la capacidad de los Estados con experiencia y establecidos, para ayudar a los Estados en desarrollo a instaurar un ciberespacio seguro, resistente y fiable, en beneficio de todos;

e) Un enfoque más coherente a la asociación con la industria para establecer directrices sobre la conducta en el ciberespacio, por ejemplo, el código de práctica de la industria de Internet de Australia.

Conceptos internacionales pertinentes

El derecho internacional vigente ofrece un marco para la protección contra amenazas a la seguridad de la información procedentes de una variedad de agentes. Algunos de los actuales principios jurídicos internacionales pueden ser aplicables a la utilización del ciberespacio, entre ellos, los principios de igualdad soberana de los Estados y la prohibición del uso de la fuerza y los actos de agresión, así como el derecho internacional humanitario. Es necesario que prosiga el debate entre los Estados, en los foros internacionales y regionales, para determinar con mayor precisión el alcance y la aplicabilidad de estos principios a las amenazas que emanan del ámbito del ciberespacio.

Estados Unidos de América

[Original: inglés]
[7 de junio de 2011]

I. Introducción

Las tecnologías de la información y las comunicaciones son vitales para el desarrollo de todos los Estados Miembros. Estas tecnologías, reunidas para crear un ciberespacio, ayudan a hacer realidad la visión común de una sociedad de la información conforme a lo previsto en las reuniones de la Cumbre Mundial sobre la Sociedad de la Información, celebradas en 2003 y 2005. Las tecnologías contribuyen a funciones esenciales de la vida cotidiana, el comercio y el suministro de bienes y servicios, la investigación, la innovación, el espíritu empresarial y la libre circulación de la información entre personas, organizaciones y gobiernos. Se trata de una herramienta nueva y poderosa, que permite el gobierno electrónico, la promoción del desarrollo económico, una prestación más fácil de la asistencia humanitaria y la habilitación de la protección pública civil y las infraestructuras fundamentales de la seguridad nacional. Por otra parte, nunca se insistirá bastante en las promesas que ofrecen las comunicaciones en red para reducir las barreras al entendimiento y la cooperación internacionales.

En la misma medida en que crece la dependencia en las TIC, crecen los riesgos asociados a esta dependencia. Una amplia gama de eventos y actividades, naturales y creados por el hombre, ponen en peligro el funcionamiento seguro de las infraestructuras nacionales críticas, las redes globales, y la integridad de la información que transportan o se almacena en su interior. Las amenazas creadas por

el hombre están aumentando en número, complejidad y gravedad. Algunas proceden de Estados, pero muchos tienen su origen en agentes no estatales, e incluyen una actividad delictiva o terrorista. Los motivos varían, desde la apropiación de dinero o información, o la perturbación causada a competidores, el nacionalismo y la extensión en el ciberespacio de las formas tradicionales de conflictos estatales. Los autores de estas amenazas las dirigen por igual contra particulares, empresas, infraestructuras nacionales críticas, y gobiernos, y sus efectos tienen consecuencias significativas para el bienestar y la seguridad de las naciones y la comunidad internacional en su conjunto interconectada con carácter mundial.

Con independencia de las medidas nacionales que puedan adoptar los gobiernos a nivel nacional para proteger sus redes de información, la colaboración internacional sobre estrategias para reducir los riesgos que penden sobre las tecnologías de la información y las comunicaciones es esencial para garantizar la seguridad de todos. Los gobiernos deben poder confiar en que las redes que sustentan su seguridad nacional y prosperidad económica son seguras y resistentes. El logro de una infraestructura de tecnologías fiable garantizará que todos puedan materializar el potencial de la revolución de la información.

Esa tarea no será fácil. La comunidad internacional enfrenta el reto de mantener un entorno que promueva la eficiencia, la innovación, la prosperidad económica y el libre comercio, a la vez que fomenta la seguridad, las libertades civiles y los derechos a la privacidad. La dificultad de la tarea se complica por los atributos peculiares de las tecnologías de la información y las comunicaciones. Accesibles a todos, las redes son a menudo de propiedad del sector privado, que las explota, y no de los gobiernos. A diferencia de las armas tradicionales, las herramientas perjudiciales de la tecnología de la información son furtivas e invisibles. Pueden atravesar por muchas naciones y es difícil determinar el origen, la identidad, y el patrocinio del autor. Algunos actores no estatales están desarrollando cada vez más capacidades que dan a los Estados o actores no estatales mayor posibilidad de utilizar sustitutos para participar en actividades perturbadoras en el ciberespacio. Debido a estos atributos, las estrategias tradicionales, como las medidas empleadas para el control de armas, sean ineficaces para controlar o limitar a los autores de la amenaza y, por tanto, se requieren nuevos enfoques creativos para mitigar los riesgos. A pesar de la dificultad de la tarea, los Estados Miembros deben unirse en el objetivo común de preservar y mejorar la contribución de las tecnologías de la información, garantizando su seguridad e integridad.

Las tareas de los Estados Miembros abarcan el ámbito nacional e internacional. La protección de las infraestructuras nacionales de información es una responsabilidad que incumbe a los gobiernos en el plano nacional, en coordinación con las partes interesadas pertinentes de la sociedad civil. Al mismo tiempo, los esfuerzos nacionales deben estar apoyados por la colaboración internacional en la concepción de estrategias que aborden la naturaleza transnacional de las diversas amenazas a los sistemas de información en red. Estos esfuerzos deben incluir la cooperación en materia de gestión de incidentes, mitigación y respuesta, investigación y enjuiciamiento penal con carácter transnacional, recomendaciones técnicas para mejorar la robustez de la infraestructura cibernética, y la afirmación de normas de conducta comunes en el plano internacional, apoyadas por medidas de fomento de la confianza destinadas a mejorar la estabilidad y reducir los riesgos de una percepción errónea.

II. Amenazas, riesgos, vulnerabilidades

Las amenazas a la red de sistemas que en conjunto constituyen el ciberespacio, y la información que transporta, es uno de los desafíos globales serios del siglo XXI. Actores estatales y no estatales pueden utilizar las tecnologías de la información y las telecomunicaciones para dirigir ataques contra particulares, el comercio, infraestructuras industriales fundamentales y los gobiernos. La convergencia entre las tecnologías, Internet y otras infraestructuras crea oportunidades sin precedentes para paralizar las telecomunicaciones, el suministro de electricidad, los oleoductos y refinerías, las redes financieras y otras infraestructuras críticas.

Las características peculiares de la tecnología de la información facilitan su uso para actividades perjudiciales e imponen un grave desafío a los gobiernos que buscan reducir el riesgo. A diferencia de las tecnologías militares, las redes que constituyen el ciberespacio no son monopolio de los gobiernos, sino en muchos casos pertenecen al sector privado y son explotadas por particulares. La propia tecnología de la información es una tecnología ampliamente disponible que no es de índole intrínsecamente civil ni militar, y su utilización depende exclusivamente de la motivación del usuario.

Los programas informáticos utilizados para perturbar las tecnologías están al alcance de todos, al menos en sus aspectos básicos. Cualquiera que tenga la habilidad necesaria puede elaborar enfoques más sofisticados. Además, estas herramientas evolucionan rápidamente para sacar partido de nuevas vulnerabilidades que se descubren. Tales instrumentos no son visibles en el sentido convencional, actúan de manera bastante furtiva, y puede tener "firmas" latentes que pueden ser fácilmente imitadas. Por la propia índole de Internet, el código malintencionado puede atravesar muchos territorios nacionales antes de llegar a la meta, por lo que la identificación de su origen es onerosa, lleva tiempo y requiere a menudo una importante cooperación transnacional. Incluso si se descubre su origen, puede seguir siendo difícil determinar la identidad del autor o de los promotores. En consecuencia, los autores malintencionados pueden operar en secreto, y lo hacen, con una impunidad sustancial, desde prácticamente cualquier lugar del planeta.

La ocultación de la identidad se ve agravada por la ocultación del motivo que inspira la intrusión en el ciberespacio. La delincuencia organizada y otros individuos o grupos pueden actuar para promover sus propios intereses, pero también pueden ser captados por actores estatales y no estatales, para que sirvan como sustitutos visibles. El hecho de que en un momento concreto no se pueda atribuir un grado elevado de confianza y pueda haber suplantación de identidad crearía incertidumbre y confusión para los gobiernos, con el consiguiente aumento del potencial de inestabilidad ante la crisis, respuestas mal orientadas y la pérdida de control de la escalada en los incidentes cibernéticos graves.

Los principales agentes que constituyen amenazas para el funcionamiento fiable del ciberespacio son:

a) **Delincuentes**. Muchas de las herramientas malintencionadas se originan en los esfuerzos de la delincuencia organizada y piratas informáticos con fines comerciales. La creciente complejidad y alcance de la actividad delictiva pone de relieve las posibilidades de que se ejecuten operaciones malintencionadas en el ciberespacio para afectar la competitividad nacional, causar un desgaste general de

confianza en el uso de Internet para el comercio y el intercambio, e incluso paralizar la infraestructura civil. El volumen y el alcance de esas actividades están en aumento;

b) **Estados**. Cada vez más el público recibe información anecdótica sobre la creación y utilización por los Estados de capacidades que extienden al ciberespacio las formas tradicionales de conflicto estatales, o lo usan con esos fines. Sin embargo, no hay aún pruebas concluyentes sobre la fuente o las intenciones que inspiran esos hechos, que comúnmente se supone promovidos por el Estado. Como suele suceder, la identidad y la motivación del autor solo se puede deducir del objetivo, los efectos, y otros indicios circunstanciales relacionados con un incidente;

c) **Terroristas**. Actualmente el terrorismo no tiene capacidad para utilizar las tecnologías de la información y las comunicaciones para poner en peligro las redes de información o ejecutar operaciones con efectos físicos, pero no puede descartarse que esas capacidades puedan surgir en el futuro. La mayoría de los expertos coinciden en que, en la actualidad, los terroristas se basan en esas tecnologías para reclutar, organizar y solicitar financiación. Entre las amenazas específicas derivadas de la utilización de Internet por terroristas figuran el uso de la Red para organizar y llevar a cabo un atentado terrorista cinético específico.

d) **Sustitutos**. Un fenómeno cada vez más preocupante es el de los individuos o grupos que ejecutan actividades malintencionadas en línea en nombre de otros, sean actores estatales o no estatales, con fines lucrativos o por motivación nacionalista o de otra índole política. Se ha informado de que los llamados “Bot-masters” ofrecen diversos servicios malintencionados al mejor postor. Por sus atributos peculiares, la tecnología de la información ofrece un alto grado de anonimato a esos actores y ocultan efectivamente cualquier relación con un patrocinador, lo que dan al promotor la posibilidad plausible de negar cualquier acusación.

Los desafíos que enfrentan los Estados en relación con estas amenazas son formidables. Por los propios atributos de las tecnologías de la información y las comunicaciones, los actos de los autores de amenaza probablemente solo serán visibles en sus efectos. Por lo tanto, la identidad de los autores no se puede determinar con un alto grado de confianza a tiempo, e incluso, nunca, y el éxito depende a menudo de un alto grado de cooperación transnacional. El creciente papel de los sustitutos complica aún más el proceso de atribución de identidad, ya que la parte afectada debe identificar no solo al autor sino también al promotor, lo que seguramente ha de agravar aún más el problema en el futuro.

Estas dificultades exigen que los gobiernos nacionales organicen y pongan en práctica actividades nacionales para crear y desplegar un sistema de defensa resistente y distribuido en varios niveles, para proteger las infraestructuras de la información y las comunicaciones, independientemente de la fuente de la amenaza. Al mismo tiempo, la compleja naturaleza transnacional de esas amenazas impone la necesidad de la colaboración internacional en la formulación de estrategias para abordar los riesgos a nivel mundial.

III. Principios, reglas y normas de conducta

A. Responsabilidades de los Estados de garantizar la seguridad del ciberespacio

En la última década, los Estados Miembros han reconocido su responsabilidad nacional de adoptar sistemáticamente medidas internas para defenderse de las amenazas a la seguridad del ciberespacio y han afirmado la necesidad de la cooperación internacional. En cinco resoluciones de la Asamblea General se ha señalado a la atención las medidas esenciales de defensa que los gobiernos puedan adoptar para reducir los riesgos a su seguridad. Aunque la intención de estas resoluciones es sensibilizar, se proponen también algunas normas útiles para regir la conducta de los particulares y el Estado en interés de la seguridad cibernética:

a) La resolución 55/63, sobre la lucha contra la utilización de la tecnología de la información con fines delictivos, en que la Asamblea General pone de relieve la necesidad de contar con una legislación nacional moderna y eficaz para enjuiciar adecuadamente los delitos informáticos y facilitar la oportuna cooperación transnacional a los fines de la investigación;

b) La resolución 56/121, en que la Asamblea General observa expresamente la labor de organizaciones internacionales y regionales en la lucha contra el delito de alta tecnología, incluida la labor del Consejo de Europa en la preparación del Convenio sobre la Ciberdelincuencia:

> Ha habido una intensa actividad de las Naciones Unidas y otras organizaciones en este ámbito. Las organizaciones de las Naciones Unidas que se centran principalmente en el uso delictivo de Internet son la Oficina de las Naciones Unidas contra la Droga y el Delito, la Comisión sobre Prevención del Delito y Justicia Penal, el Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, la Unión Internacional de Telecomunicaciones, y otros.

c) La resolución 57/239, en que la Asamblea General afirma la necesidad de una cultura de seguridad cibernética, reconoce la responsabilidad de los gobiernos de contribuir a que todos los elementos de la sociedad entiendan sus funciones y responsabilidades con respecto a la seguridad cibernética, y pone de relieve los elementos complementarios que todos los participantes en la sociedad de la información deben tomar en consideración;

d) La resolución 58/199, en que la Asamblea General se centra en particular en las acciones que los Estados miembros deben considerar en sus esfuerzos por crear una cultura global de seguridad cibernética y proteger las infraestructuras de información críticas. Estas también pueden considerarse un conjunto de normas a las que los gobiernos deben suscribir, y proporcionan una base o precursor esencial para facilitar la colaboración internacional en la reducción del riesgo;

e) La resolución 64/211 en que la Asamblea General invita a todos los Estados miembros a hacer un balance detallado de sus esfuerzos nacionales hasta la fecha en materia de seguridad cibernética, en los ámbitos antes mencionados, así como en otros, con utilización de un instrumento de autoevaluación que figura en anexo, y a compartir las medidas y mejores prácticas eficaces que puedan ayudar a otros Estados Miembros en sus esfuerzos.

B. Normas aplicables en el contexto de las hostilidades

A pesar de que las tecnologías de la información tienen atributos peculiares, los principios actuales del derecho internacional sirven de marco adecuado para identificar y analizar las reglas y normas de conducta que deben regir el uso del ciberespacio en relación con las hostilidades. A este respecto se deben considerar dos cuerpos de legislación distintos pero relacionados entre sí: *jus ad bellum* y *jus in bello*. El primer concepto proporciona el marco para considerar si un incidente en el ciberespacio alcanza el nivel de uso de la fuerza que da a una nación el derecho a la legítima defensa. El segundo proporciona el marco para determinar las normas que rigen el uso del ciberespacio en el contexto de un conflicto armado.

Jus ad bellum. Gran parte del marco jurídico que rige el uso de la fuerza y la legítima defensa deriva de tres disposiciones de la Carta de las Naciones Unidas:

a) El artículo 2 4) de la Carta de las Naciones Unidas establece que "[l]os Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado ...";

b) El artículo 39 de la Carta establece que el Consejo de Seguridad determinará como árbitro la existencia de toda amenaza a la paz, quebrantamiento de la paz o acto de agresión y hará recomendaciones o decidirá qué medidas de conformidad con los Artículos 41 y 42 de la Carta constituirían una respuesta apropiada;

c) El artículo 51 de la Carta reconoce y refuerza el principio de que "[n]inguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales".

Puede ser difícil llegar a una conclusión jurídica definitiva sobre si una actividad perjudicial en el ciberespacio constituye un ataque armado que activa el derecho a la legítima defensa. Por ejemplo, cuando se desconoce al autor de la amenaza y el motivo, y los efectos no causan directamente la muerte o una destrucción física importante, es posible que se llegue a conclusiones divergentes a la hora de determinar si se ha producido un ataque armado. Sin embargo, tal ambigüedad y margen para la discrepancia no indica que sea necesario establecer un nuevo marco jurídico específico para el ciberespacio. En cambio, simplemente reflejan las dificultades que se plantean en la aplicación del marco de la Carta, que ya existen en muchos contextos. Sin embargo, en algunas circunstancias, una actividad perturbadora en el ciberespacio podría constituir un ataque armado. En ese contexto, se aplicarán los siguientes principios establecidos:

a) El derecho a la legítima defensa contra un ataque armado inminente o en curso se aplica si el atacante es un agente estatal o un agente no estatal;

b) El uso de la fuerza en legítima defensa debe limitarse a lo necesario para hacer frente a un ataque armado inminente o en curso y debe ser proporcional a la amenaza que se plantea;

c) Los Estados están obligados a adoptar todas las medidas necesarias para garantizar que sus territorios no sean utilizados por otros Estados o actores no estatales a los efectos de actividades armadas, lo que incluye planificación,

amenaza, comisión o prestación de apoyo material para ataques armados contra otros Estados y sus intereses.

Jus in bello. El derecho aplicable a los conflictos armados establece las reglas, conocidas como *jus in bello*, que se aplican al desarrollo de los conflictos armados, como el uso de herramientas de la tecnología de la información en el contexto de un conflicto armado. En particular, los siguientes principios fundamentales del derecho aplicable a los conflictos armados contribuirían considerablemente a la hora de juzgar la legalidad de los ataques cibernéticos durante un conflicto armado:

a) El principio de distinción requiere que los ataques se limiten a objetivos militares legítimos, y que los bienes de carácter civil no sean objeto de ataque;

b) La prohibición de ataques indiscriminados incluye la prohibición de los ataques que emplean medios o métodos de combate que no pueden razonablemente dirigirse contra un objetivo militar concreto;

c) El principio de proporcionalidad prohíbe los ataques que puedan causar de forma incidental muertos y heridos entre la población civil, o daños a bienes de carácter civil, o ambas cosas, que sean excesivos en relación con la ventaja militar concreta y directa prevista.

Estos principios prohíben los ataques a la infraestructura de carácter exclusivamente civil, cuando la perturbación o la destrucción resultante no producirían ninguna ventaja militar significativa. Además, antes de atacar un objetivo militar se debe evaluar la posibilidad de daños colaterales. En otras palabras, en el caso de ataques con utilización de la tecnología de la información deberían llevarse a cabo análisis sobre el objetivo, del mismo modo que tradicionalmente se han llevado a cabo esos análisis para los ataques con armas cinéticas (convencionales y estratégicas).

Si bien los principios mencionados están bien establecidos y se aplican en el contexto del ciberespacio, también es cierto que la interpretación de estos cuerpos de legislación en el contexto de las actividades en el ciberespacio puede presentar desafíos nuevos y peculiares que requieren la consulta y la cooperación entre las naciones. Esto no es poco habitual. Cuando se desarrollan nuevas tecnologías, a menudo se plantean problemas en la aplicación del conjunto normativo en vigor.

C. Utilización de sustitutos

El uso de sustitutos para llevar a cabo operaciones de perturbación ilustra un ámbito en que los atributos peculiares de la tecnología de la información y las comunicaciones plantean nuevos retos para los Estados. La actuación a través de sustitutos aumenta significativamente la capacidad de los Estados de participar en ataques, con la posibilidad de negarlo de forma plausible. Aunque el derecho internacional en vigor contiene disposiciones que rigen la utilización de mercenarios, el uso de sustitutos en el ciberespacio plantea problemas nuevos e importantes con consecuencias de amplio alcance. Los Estados tendrán que trabajar juntos para desarrollar soluciones efectivas para este problema.

D. Responsabilidad para permitir la libre circulación de la información

El derecho a la libertad de expresión y la libre circulación de la información están consagrados en la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos, que establecen en general, sujeto a ciertas limitaciones, que toda persona tiene derecho a la libertad de expresión, incluida la libertad de emitir opiniones sin injerencia y buscar, recibir e impartir información por cualquier medio y sin consideración de fronteras. Estos principios se han reafirmado en numerosos foros internacionales, en particular, la Asamblea General, la Unión Internacional de Telecomunicaciones, y la Cumbre Mundial sobre la Sociedad de la Información, entre otros.

E. Responsabilidad de combatir el terrorismo

Al menos 16 resoluciones en vigor del Consejo de Seguridad imponen a los Estados la lucha contra el terrorismo. Esta obligación se aplica plenamente cuando los terroristas o promotores de terroristas utilizan el ciberespacio para reclutar, recaudar fondos y transferir dinero, adquirir armas, y planear ataques. Todos los Estados están obligados a compartir información acerca de las actividades en línea para la financiación, el reclutamiento, la planificación y la facilitación del terrorismo, y tomar medidas para combatirlas, respetando la soberanía de los otros Estados y sus propias responsabilidades para permitir la libre circulación de la información.

IV. Transparencia, estabilidad y reducción del riesgo y medidas de cooperación

Como se mencionó anteriormente, los Estados miembros hacen frente al reto de gestionar un entorno de amenazas muy variadas y complejas. Durante la última década, se han desplegado grandes esfuerzos a nivel internacional para combatir la amenaza de la ciberdelincuencia. La Organización de Estados Americanos, el Foro de Cooperación Económica Asia-Pacífico, la Comunidad Económica de Estados de África Occidental, la Unión Africana y el Consejo de Europa, entre otros, han tomado medidas en materia de formación, investigación y enjuiciamiento de la ciberdelincuencia. Se ha logrado una amplia cooperación internacional en la investigación y enjuiciamiento de los delitos cibernéticos a través del Convenio sobre la Ciberdelincuencia, así como por conducto de los esfuerzos bilaterales entre los países afectados, y esta sigue siendo la forma más eficaz de hacer frente a las amenazas a la tecnología de la información y las comunicaciones que plantean las actividades delictivas.

Otros ámbitos de interés transnacional aún no han recibido una atención similar. Estos incluyen los riesgos de la percepción errónea que resultan de una falta de entendimiento común de las normas internacionales relativas a la conducta del Estado en el ciberespacio, lo que podría afectar a la gestión de crisis en caso de incidentes cibernéticos importantes. Ello aboga por la elaboración de medidas destinadas a mejorar la cooperación y fomentar la confianza, reducir el riesgo, o aumentar la transparencia y la estabilidad:

Medidas de transparencia

- Intercambio de información sobre estrategias nacionales y mejores prácticas (enseñanzas aprendidas) en materia de seguridad cibernética
- Intercambios de los puntos de vista nacionales de las normas internacionales que rigen el uso del ciberespacio
- Intercambios de información acerca de las estructuras institucionales nacionales dedicadas a la seguridad cibernética y puntos de contacto.

Medidas de estabilidad y de reducción del riesgo

- Establecimiento o mejoramiento de los enlaces de comunicaciones y protocolos asociados para abarcar los incidentes cibernéticos
- Mejoramiento de la cooperación para hacer frente a actores no estatales organizados (delincuentes, terroristas, sustitutos)
- Establecimiento de procedimientos que permitan un intercambio regular de información entre los equipos de respuesta a incidentes de seguridad informática.

Medidas de cooperación

- Apoyo a la creación de capacidad en seguridad cibernética en los países menos desarrollados

Georgia

[Original: inglés]
[1 de junio de 2011]

En el contexto de Georgia, se prestó especial atención a los problemas de seguridad de la información a partir de agosto de 2008, fecha en que la Federación de Rusia llevó a cabo intensos ataques de "denegación de servicio" contra Georgia.

A raíz de la evaluación de esos eventos y en virtud de la reciente evolución rápida y en gran escala de los proyectos y servicios de gobierno electrónico, la seguridad de la información se ha convertido en uno de los aspectos importantes del concepto de seguridad nacional. Para una mejor reglamentación de la seguridad de la información, en los últimos años el Gobierno de Georgia ha emprendido una serie de iniciativas importantes.

En 2010 se creó en el Ministerio de Justicia de Georgia una entidad jurídica, la Agencia de intercambio de datos, que es directamente responsable de la elaboración y ejecución de la política de seguridad de la información en el sector gubernamental. Con la creación de esa Agencia, el Gobierno de Georgia ha establecido el mecanismo institucional para poner en práctica, de forma coordinada, el gobierno electrónico y la seguridad de la información.

La Agencia de intercambio de datos, dentro del marco de las funciones previstas por la ley y su propia Carta, colabora con el Ministerio de Justicia de Georgia en la aplicación e introducción de la política de seguridad de la información, que deberá ajustarse a la norma ISO 27000 de la Organización

Internacional de Normalización. La Agencia también coordina la aplicación y la introducción de todos los mecanismos o normas necesarios para la seguridad de la información en los sectores estatal y empresarial, en particular, mediante la realización de actividades de diversos niveles de importancia. De estos eventos, uno de los principales es la Conferencia anual de innovaciones en tecnología de la información de Georgia, en cuyo programa siempre figura la información y la seguridad cibernética; la Conferencia también tiene mandato de la Agencia para formular y aplicar la política de sensibilización pública respecto de las cuestiones de información y seguridad cibernética.

En el contexto de la seguridad cibernética en la vida cotidiana, la Agencia de intercambio de datos es responsable de la creación y el funcionamiento del equipo de respuesta ante emergencias informáticas, que actualmente opera dentro de la institución para abordar los incidentes de seguridad de la información en el ciberespacio de Georgia. La Agencia también supervisa el funcionamiento de la Red del Gobierno de Georgia para la protección de su seguridad.

Entre las funciones de la Agencia en el contexto de la información y las comunicaciones figura también aumentar el nivel de educación profesional (con el fin de formar a especialistas en seguridad de información), la preparación de propuestas, el control de la seguridad y la emisión de certificados de firma digital. Teniendo en cuenta el alcance de la formación profesional, la Agencia tiene previsto llevar a cabo una serie de proyectos especiales con la ayuda de los donantes internacionales (por ejemplo, la Unión Europea (UE) y el Banco Mundial). Estos proyectos han de garantizar que se imparta el nivel adecuado de formación profesional; en cuanto a la seguridad de la firma digital, la Agencia se ocupará de esta función una vez que la Oficina de Registro Civil comience a emitir tarjetas de identidad electrónica para los ciudadanos (que lleven firmas digitales).

Además de la actividad de la Agencia de intercambio de datos, que es el principal organismo de coordinación para la seguridad de la información, se deben destacar otras iniciativas del Gobierno de Georgia actualmente en curso, en que la Agencia de intercambio de datos participa activamente:

a) En el marco del Consejo de Seguridad Nacional de Georgia se ha establecido un grupo de trabajo de expertos, que se ocupa de formular la estrategia de seguridad cibernética y el plan de acción (que se define concretamente en la parte siguiente);

b) Se ha estado trabajando en una serie de iniciativas legislativas, como la normativa de derecho administrativo y la ley que rige el secreto de Estado, que según lo previsto se comenzarán a examinar en el Parlamento de Georgia en 2011. Merece una mención especial el proyecto de ley sobre seguridad de la información, que prepara actualmente la Agencia de intercambio de datos y que será sometido a consideración del Parlamento en 2011;

c) En 2010 el Ministerio de Justicia y el Ministerio de Finanzas de Georgia, con la ayuda de la Agencia, prepararon el reglamento interno de la seguridad de la información (políticas y directrices), que están introduciendo actualmente. Se prevén asimismo iniciativas similares que han de ser puestas en práctica en otras instituciones gubernamentales.

Grecia

[Original: inglés]
[6 de junio de 2011]

Las cuestiones relativas a la seguridad de la información se abordan con mayor profundidad que antes. Se examinan las medidas para hacer frente a las amenazas inherentes a la globalización actual de las redes y los sistemas. Se estudian medidas para preservar la libre circulación de información, que se aplican en el contexto nacional y transfronterizo.

Se hace un seguimiento y estudio de los actuales conceptos internacionales y multinacionales. Se requiere orientación internacional en materia de evaluación de los riesgos. También debe abordarse la cuestión de la defensa cibernética. Deben mantenerse los derechos de soberanía nacional en relación con la seguridad informática en el contexto del intercambio mundial de información.

Se entiende que todos los Estados Miembros deben continuar transmitiendo al Secretario General sus opiniones y evaluaciones en relación con las cuestiones pertinentes. A este respecto, se señalan los siguientes aspectos:

a) Se atribuye alta prioridad a todas las cuestiones relativas a la seguridad de la información en general;

b) Se estudian y aplican los medios para mantener la corriente de información y garantizar el grado necesario de confidencialidad, integridad y accesibilidad a nivel nacional y a través de las fronteras internacionales;

c) Se debe elaborar y acordar una base conceptual para la interconexión de redes que garantice que las capacidades se utilicen e intercambien a nivel nacional e internacional. Se debe velar por que se evalúen los riesgos para la interconexión de redes y asegurar el acceso a asesoramiento internacional pertinente. Además, dado que la necesidad de tomar medidas de defensa cibernética es motivo de gran preocupación para todos los países, se requiere una orientación internacional coherente a efectos de cooperación, eficiencia y economía. Por último, no se debe pasar por alto la necesidad de que los países preserven su soberanía y mantengan su propia base de información, y esto debe tenerse en cuenta en todos los conceptos que se elaboren;

d) A continuación se enumeran las posibles medidas que debería adoptar la comunidad internacional para fortalecer la seguridad de la información a nivel mundial:

i) Elaborar en detalle los conceptos internacionales pertinentes y convenir en ellos;

ii) Proponer un plan de orientación para crear una infraestructura general armonizada que abarque las cuestiones básicas en materia de legislación a fin de garantizar la seguridad de la información necesaria para la manipulación electrónica de toda la correspondencia y los mensajes, facilitando los diversos modos de comunicación;

iii) Armonizar y ampliar conceptos que sirvan de guía a las alianzas multinacionales y pequeñas agrupaciones de países a fin de que sean aplicables a nivel mundial. Llegar a un acuerdo en lo que respecta a determinar la amenaza y sus efectos negativos podría ser más importante que elaborar

medidas complejas, ya que estas últimas también podrían ser utilizadas por los adversarios;

iv) Al mismo tiempo, la soberanía nacional debe servir de referencia básica en todo intento de globalización. Se debe elaborar un concepto internacional a fin de definir los portales nacionales para el intercambio de información con marcos hipotéticos que reflejen el nivel deseado de integración para todas las actividades a nivel nacional, internacional y multinacional.

Kazajstán

[Original: ruso]
[7 de junio de 2011]

En 2010, la República de Kazajstán creó un equipo de respuesta para emergencias informáticas con el objetivo de garantizar la seguridad cibernética de las tecnologías de la información y las comunicaciones.

En este sentido, se envía al equipo de respuesta para emergencias informáticas, para su análisis, toda información recibida de usuarios de internet de o relacionados con Kazajstán y relativa a detecciones de virus, códigos de seguridad, programas para la creación de sistemas robot y violaciones de la legislación pertinente (pornografía, violencia, violación de los derechos de autor, etc.) que se den en el dominio KZ o en un alojamiento web kazajo.

Países Bajos

[Original: inglés]
[6 de junio de 2011]

Evaluación general de los problemas de la seguridad de la información

Los Países Bajos manifiestan su apoyo a la seguridad y fiabilidad de la tecnología de la información, y subrayan la necesidad de proteger una red Internet libre y abierta, en el respeto de los derechos humanos. La seguridad y fiabilidad de las tecnologías de la información y de las comunicaciones son esenciales para nuestra prosperidad y bienestar, pues esas tecnologías actúan como catalizador del crecimiento económico sostenible.

Tales tecnologías ofrecen oportunidades, pero también hacen nuestra sociedad más vulnerable. El carácter transfronterizo de las amenazas subraya la necesidad de la cooperación internacional. Muchas de las medidas sólo serán eficaces si se aplican o están coordinadas en el plano internacional. En ese sentido, los Países Bajos consideran muy importantes las asociaciones de los sectores público y privado y la responsabilidad individual de todos los usuarios de las tecnologías.

Medidas que se adoptan a nivel nacional para fortalecer la seguridad de la información y contribuir a la colaboración internacional en ese ámbito

Los Países Bajos trabajan a nivel nacional e internacional para crear un entorno digital seguro. A nivel nacional, en febrero de 2011 el Gobierno de los Países Bajos presentó una Estrategia nacional de seguridad cibernética, titulada "La fuerza a través de la cooperación". En julio de 2011, como parte de esta estrategia, el Gobierno establecerá un Consejo nacional de seguridad cibernética para asegurar un enfoque de colaboración entre el sector público, el sector privado y las instituciones académicas y de investigación. El Gobierno también creará un Centro nacional de seguridad cibernética para identificar las tendencias y las amenazas y ayudar a abordar los incidentes y crisis. Una de las principales tareas del Centro será la de analizar las amenazas cibernéticas sobre la base de información de las partes públicas y privadas. El Centro incluirá al actual equipo nacional de respuesta ante emergencias informáticas del Gobierno.

A nivel internacional los Países Bajos contribuyen activamente los esfuerzos de la UE, la OTAN, el Foro para la Gobernanza de Internet, la UIT y otras asociaciones. Promueven la cooperación práctica entre los centros que se ocupan de la seguridad cibernética (incluidas las organizaciones de equipos de respuesta ante emergencias informáticas) y el fortalecimiento de la Red de alerta y vigilancia internacional. El rápido crecimiento de la ciberdelincuencia exhorta a velar por una aplicación efectiva de la ley para mantener la confianza en la sociedad digital. En lo que respecta a esa aplicación efectiva, los Países Bajos tienen como objetivo fomentar una mayor investigación transfronteriza con las autoridades de otros países europeos y de otras regiones. El país es parte en el Convenio del Consejo de Europa sobre la Ciberdelincuencia y alienta a otros a adherirse a este Convenio.

Posibles medidas que podría adoptar la comunidad internacional para fortalecer la seguridad de la información a nivel mundial

Los Países Bajos son conscientes de la importancia de continuar el diálogo sobre la elaboración de normas de conducta del Estado con miras a una utilización segura del ciberespacio, y están dispuestos a contribuir activamente en este diálogo. Para el país, el punto de partida es una Internet abierta que promueva la innovación, estimule el crecimiento económico y proteja las libertades fundamentales.

Los Países Bajos conceden gran importancia a la participación del sector privado y las instituciones del conocimiento en este diálogo, y están dispuestos a compartir con otros sus experiencias y mejores prácticas

Para que el ciberespacio sea más seguro y confiable, es esencial un intenso intercambio internacional de conocimientos e información entre todas las partes interesadas y las organizaciones. La coherencia en la aplicación de los marcos jurídicos internacionales es otro tema importante que merece la atención internacional.